

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for enforcing a plurality of different policies on a stream of packets, the method comprising:

receiving a packet in a packet-switched network;

appending an extension to the packet;

determining session information regarding the packet;

updating the extension with the session information;

forwarding the packet to a packet policy rule engine module;

determining, at the packet policy rule engine module, whether the packet corresponds to a common condition for a first policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type;

providing, at the packet policy rule engine module, an association between the first packet and the common condition where it is determined that the packet corresponds to the common condition; and

updating the extension with the association, wherein communication between modules of said packet-switched network using said extension occurs without use of shared memory.
2. (Previously Presented) The method of claim 1, further comprising:

forwarding the packet to an application decode engine module;

determining, at the application engine decode module, whether the packet corresponds to an application rule;

if the packet corresponds to an application rule, at the application engine decode module, updating the extension with application information from the application rule; and

wherein said forwarding the packet to a packet policy rule engine module includes

forwarding the packet from the application engine decode module to a packet policy rule engine module.

3. (Original) The method of claim 1, further comprising:

determining whether the packet corresponds to a first particular condition for the first policy rule as compared to the second policy rule; and

determining applicability of the first policy rule to the packet where it is determined that the common condition and the first particular condition correspond to the packet.

4. (Previously Presented) The method of claim 1, wherein said appending an extension to the packet occurs at an extension builder module.

5. (Original) The method of claim 3, wherein determining applicability of the first policy rule to the packet comprises:

traversing a rule tree corresponding to the first policy rule, the rule tree having a first path corresponding to the first rule, the first path including the common condition and the first particular condition, wherein presence of the common condition and the first

particular condition prompts a determination that the first policy rule is applicable to the packet.

6. (Original) The method of claim 1, wherein the first policy type is a firewall policy and the second policy type is a quality of service policy.
7. (Original) The method of claim 1, wherein the first and second policy types are selected from the following policy types: firewall, quality of service, intrusion detection.
8. (Previously Presented) The method of claim 4, wherein said determining session information regarding the packet and said updating the extension with the session information occur at a session manager module.
- 9-13. (Canceled)
14. (Currently Amended) An apparatus for enforcing a plurality of different policies on a stream of packets, the apparatus comprising:
 - means for receiving a packet in a packet-switched network;
 - means for appending an extension to the packet;
 - means for determining session information regarding the packet;
 - means for updating the extension with the session information;
 - means for forwarding the packet to a packet policy rule engine module;

means for determining, at the packet policy rule engine module, whether the packet corresponds to a common condition for a first policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type;

means for providing, at the packet policy rule engine module, an association between the first packet and the common condition where it is determined that the packet corresponds to the common condition; and

means for updating the extension with the association, wherein communication between modules of said packet-switched network using said extension occurs without use of shared memory.

15. (Previously Presented) The apparatus of claim 14, further comprising:

means for forwarding the packet to an application decode engine module;

means for determining, at the application engine decode module, whether the packet corresponds to an application rule;

means for, if the packet corresponds to an application rule, at the application engine decode module, updating the extension with application information from the application rule;

and

wherein said means for forwarding the packet to a packet policy rule engine module includes means for forwarding the packet from the application engine decode module to a packet policy rule engine module.

16. (Original) The apparatus of claim 14, further comprising:

means for determining whether the packet corresponds to a first particular condition for the first policy rule as compared to the second policy rule, determining applicability of the first policy rule to the packet where it is determined that the common condition and the first particular condition correspond to the packet.

17. (Previously Presented) The apparatus of claim 14, wherein said means for appending an extension to the packet builder includes an extension builder module.
18. (Original) The apparatus of claim 16, wherein determining applicability of the first policy rule to the packet comprises traversing a rule tree corresponding to the first policy rule, the rule tree having a first path corresponding to the first rule, the first path including the common condition and the first particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet.
19. (Original) The apparatus of claim 14, wherein the first policy type is a firewall policy and the second policy type is a quality of service policy.
20. (Original) The apparatus of claim 14, wherein the first and second policy types are selected from the following policy types: firewall, quality of service, intrusion detection.

21. (Previously Presented) The apparatus of claim 17 wherein said means for determining session information regarding the packet and said means for updating the extension with the session information include a session manager module.

22-26. (Canceled)

27. (Currently Amended) An apparatus for enforcing a plurality of different policies on a stream of packets, the apparatus comprising:

an extension builder module configured to receive a packet in a packet-switched network, appending an extension to the packet, and forward the packet to a session manager module;

said session manager module configured to receive the packet, determine session information regarding the packet, update the extension with the session information, and forward the packet to an application decode engine module;

said application decode engine module configured to determine if the packet corresponds to an application rule, update the extension with application information from the application if the packet corresponds to an application rule, and forward the packet to a packet policy rule engine module; and

said packet policy rule engine module configured to determine whether the packet corresponds to a common condition for a first policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type, provide an association between the first packet and the common condition where it is determined that the packet

corresponds to the common condition, and update the extension with the association,
wherein communication between modules of said packet-switched network using said
extension occurs without use of shared memory.

28. (Canceled)

29. (Previously Presented) The apparatus of claim 27, wherein said packet policy rule engine module is further configured to:

determine whether the packet corresponds to a first particular condition for the first policy rule as compared to the second policy rule; and

determine applicability of the first policy rule to the packet where it is determined that the common condition and the first particular condition correspond to the packet.

30. (Canceled)

31. (Previously Presented) The apparatus of claim 29, wherein the packet policy rule engine module is further configured to traverse a rule tree corresponding to the first policy rule, the rule tree having a first path corresponding to the first rule, the first path including the common condition and the first particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet.

32. (Original) The apparatus of claim 27, wherein the first policy type is a firewall policy and the second policy type is a quality of service policy.
33. (Original) The apparatus of claim 27, wherein the first and second policy types are selected from the following policy types: firewall, quality of service, intrusion detection.
- 34-39. (Canceled)
40. (New) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method for enforcing a plurality of different policies on a stream of packets, the method comprising:
- receiving a packet in a packet-switched network;
 - appending an extension to the packet;
 - determining session information regarding the packet;
 - updating the extension with the session information;
 - forwarding the packet to a packet policy rule engine module;
 - determining, at the packet policy rule engine module, whether the packet corresponds to a common condition for a first policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type;
 - providing, at the packet policy rule engine module, an association between the first packet and the common condition where it is determined that the packet corresponds to the common condition; and

updating the extension with the association, wherein communication between modules of
said packet-switched network using said extension occurs without use of shared
memory.